UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/605,061	09/05/2003	David S. Colvin	COL404PUS	2060

36547 7590 03/17/2008
BIR LAW, PLC
13092 GLASGOW CT.
PLYMOUTH, MI 48170-5241

EXAMINER	
REVAK, CHRISTOPHER A	
ART UNIT	PAPER NUMBER
2131	
MAIL DATE	DELIVERY MODE
03/17/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/605,061	COLVIN, DAVID S.	
	Examiner	Art Unit	
	Christopher A. Revak	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12/5/07*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *12/5/07* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-99* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *6/25/03* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. In view of the appeal brief filed on December 5, 2007, PROSECUTION IS HEREBY REOPENED. A new grounds of rejection is set forth below.

To avoid abandonment of the application, appellant must exercise one of the following two options:

(1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply under 37 CFR 1.113 (if this Office action is final); or,

(2) initiate a new appeal by filing a notice of appeal under 37 CFR 41.31 followed by an appeal brief under 37 CFR 41.37. The previously paid notice of appeal fee and appeal brief fee can be applied to the new appeal. If, however, the appeal fees set forth in 37 CFR 41.20 have been increased since they were previously paid, then appellant must pay the difference between the increased fees and the amount previously paid.

A Supervisory Patent Examiner (SPE) has approved of reopening prosecution by signing below:

/Ayaz R. Sheikh/

Supervisory Patent Examiner, Art Unit 2131

Response to Arguments

2. Applicant's arguments with respect to claims 1-99 have been considered but are moot in view of the new grounds of rejection.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-25,29-32,35-56,58-65,67-70, and 72-77 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ananda, U.S. Patent 5,495,411 in view of Xu et al, U.S. Patent 6,915,425 in further view of Slama, U.S. Patent 6,665,799.

As per claim 1, Ananda teaches of a method for securing software to reduce unauthorized use, the method comprising providing at least one authorized representative entity; obtaining registration information corresponding to at least one user device; generating an authentication code at least partially based on the registration information; associating the authentication code with the software; determining whether a current user device is authorized based on the authentication code associated with the software and registration information associated with the current user device; and controlling access to the software based on whether the current user device is authorized (col. 3, lines 11-15 & 21-28; col. 4, lines 18-28; and col. 11, lines 9-13). The teachings of Ananda disclose of a continuous connection to the remote authorized representative entity, but fail to teach that the continuous connection to a remote authorized entity is not required and that the authorized representative entity is installed in or on the user device. It is taught by Xu et al of permitting offline (non-continuous connection) playback of digital content files which includes managing the related content rights (col. 2, lines 23-24). Keys are retrieved by the end user's

system and a license (authorized representative entity) is retrieved from a license server which is installed on the end user's system, the license is required for playback of the content file (col. 3, lines 11-19 and col. 5, lines 24-38). It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to apply localized validation of licensed software. The teachings of Xu et al disclose of motivation for applying localized validation by reciting of the need to protect digital information and management of digital rights in an offline environment (col. 2, lines 15-19). It is obvious that the teachings of Ananda would have benefited from validation of licensed software by using the authorized representative installed in or on the user's device whereby the authorized representative would then be able to valid the use of licensed software offline on an enduser's system as taught by Xu et al.

The combined teachings of Ananda and Xu et al fail to disclose that the authorized representative entity is hardware. It is taught by Slama of using a hardware based authorized representative entity that is installed on a computer (col. 3, lines 47-54 and col. 11, lines 53-56). It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to apply hardware based protection. The teachings of Slama recite of motivation of using a dedicated device to ensure that protected software is only executed on authorized computers (col. 2, lines 9-15). It is obvious that the combined teachings of Ananda and Xu et al would have been further secured from unauthorized usage by requiring a hardware based representative to be used in order to dictate if software is authorized for execution on a particular computer as is disclosed by Slama.

As per claims 2 and 42, Ananda discloses wherein the software is self activating and self authenticating in conjunction with the authorized (col. 10, lines 4-15). The teachings of Xu et al are relied upon for disclosing of the permitting offline (non-continuous connection) playback of digital content files which includes managing the related content rights (col. 2, lines 23-24), please refer above for the motivation of applying the aspect of offline validation as is disclosed by Xu et al. Slama is relied upon for disclosing of the use of a hardware based authorized representative entity that is installed on a computer (col. 3, lines 47-54 and col. 11, lines 53-56), please refer above for the motivation of applying the teachings of Slama.

As per claim 3, it is taught by Ananda wherein the software comprises data representing content selected from the group consisting of music, video, an application program, an operating system component, a game, a movie, graphics, watermarked works, a magazine, and a book (col. 1, lines 17-19).

As per claim 4, it is disclosed by Ananda wherein the step of obtaining registration information is at least partially performed by the authorized representative entity (col. 3, lines 21-29). The teachings of Xu et al are relied upon for disclosing of the permitting offline (non-continuous connection) playback of digital content files which includes managing the related content rights (col. 2, lines 23-24), please refer above for the motivation of applying the aspect of offline validation as is disclosed by Xu et al. Slama is relied upon for disclosing of the use of a hardware based authorized representative entity that is installed on a computer (col. 3, lines 47-54 and col. 11, lines 53-56), please refer above for the motivation of applying the teachings of Slama.

As per claim 5, it is taught by Ananda wherein the step of generating an authentication code is at least partially performed by the authorized representative (col. 4, lines 39-46). The teachings of Xu et al are relied upon for disclosing of the permitting offline (non-continuous connection) playback of digital content files which includes managing the related content rights (col. 2, lines 23-24), please refer above for the motivation of applying the aspect of offline validation as is disclosed by Xu et al. Slama is relied upon for disclosing of the use of a hardware based authorized representative entity that is installed on a computer (col. 3, lines 47-54 and col. 11, lines 53-56), please refer above for the motivation of applying the teachings of Slama.

As per claim 6, Ananda teaches wherein the step of obtaining registration information is performed by a remotely located authorized representative entity (col. 1, lines 17-19 and col. 11, lines 61-65).

As per claim 7, Ananda discloses wherein the step of generating an authentication code is performed by a remotely located authorized representative entity (col. 11, lines 9-13).

As per claim 8, it is taught by Ananda wherein the steps of obtaining, generating, associating, determining, and controlling are at least partially performed by a resident authorized representative entity (col. 10, lines 4-15 and col. 11, lines 61-65). The teachings of Xu et al are relied upon for disclosing of the permitting offline (non-continuous connection) playback of digital content files which includes managing the related content rights (col. 2, lines 23-24), please refer above for the motivation of applying the aspect of offline validation as is disclosed by Xu et al. Slama is relied upon

for disclosing of the use of a hardware based authorized representative entity that is installed on a computer (col. 3, lines 47-54 and col. 11, lines 53-56), please refer above for the motivation of applying the teachings of Slama.

As per claim 9, it is disclosed by Ananda wherein registration information associated with the current user device remains within a trusted network associated with the user device (col. 3, lines 16-29).

As per claim 10, Ananda teaches wherein registration information associated with the current user device is not communicated to any third party (col. 3, lines 16-29).

As per claim 11, Ananda discloses wherein the steps of obtaining registration information, generating an authentication code, and associating the authentication code are performed prior to transferring the software to the current user device (col. 3, lines 16-49).

As per claim 12, it is taught by Ananda wherein the steps of obtaining registration information, generating an authentication code, and associating the authentication code are performed substantially concurrently with transferring the software to the current user device (col. 3, lines 16-49 and col. 4, lines 39-48).

As per claim 13, it is disclosed by Ananda wherein the steps of obtaining registration information, generating an authentication code, and associating the authentication code are performed following transferring the software to the current user device (col. 3, lines 16-49 and col. 10, lines 8-15).

As per claim 14, Ananda teaches wherein the steps of obtaining, generating, and associating are performed by a remote authorized representative entity (col. 10, lines 8-15).

As per claims 15-21 and 44-50, the teachings of Xu et al are relied upon for disclosing of the permitting offline (non-continuous connection) playback of digital content files which includes managing the related content rights (col. 2, lines 23-24), please refer above for the motivation of applying the aspect of offline validation as is disclosed by Xu et al. The teachings of Xu et al disclose of the authorized representative entity being software, but the combined teachings of Ananda and Xu et al fail to disclose of the authorized representative entity comprises a hardware device such as a computer chip, hardware device integral with a CPU, a PC card, or a microprocessor which included hard coded and programmable functions. It is taught by Slama of using a hardware based authorized representative entity that is installed on a computer which is a computer chip, hardware device integral with a CPU, a PC card and a microprocessor which included hard coded and programmable functions (col. 3, lines 47-54 and col. 11, lines 53-56). It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to apply hardware based protection. The teachings of Slama recite of motivation of using a dedicated device to ensure that protected software is only executed on authorized computers (col. 2, lines 9-15). It is obvious that the combined teachings of Ananda and Xu et al would have been further secured from unauthorized usage by requiring a

hardware based representative to be used in order to dictate if software is authorized for execution on a particular computer as is disclosed by Slama.

As per claim 22, Ananda teaches wherein the steps of determining whether a current user device is authorized and controlling access to the software are at least partially performed by the hardware representative entity (col. 10, lines 4-15 and col. 11, lines 61-65). The teachings of Xu et al are relied upon for disclosing of the permitting offline (non-continuous connection) playback of digital content files which includes managing the related content rights (col. 2, lines 23-24), please refer above for the motivation of applying the aspect of offline validation as is disclosed by Xu et al. Slama is relied upon for disclosing of the use of a hardware based authorized representative entity that is installed on a computer (col. 3, lines 47-54 and col. 11, lines 53-56), please refer above for the motivation of applying the teachings of Slama.

As per claim 23, Ananda discloses wherein the software is electronically distributed (col. 9, lines 35-36).

As per claim 24, it is taught by Ananda wherein the software is transferred to a user device from a computer readable storage medium (col. 6, lines 57-63 and col. 9, lines 35-36).

As per claim 25, it is disclosed by Ananda wherein at least one authentication code is distributed with the software (col. 3, lines 11-15).

As per claim 29, Ananda teaches wherein the authentication code at least partially corresponds to a unique user device (col. 3, lines 11-15).

As per claim 30, Ananda discloses wherein the steps of determining whether a current user device is authorized and controlling access to the software are performed by a remotely located authorized representative entity (col. 3, lines 16-49).

As per claim 31, it is taught by Ananda wherein the step of controlling access to the software comprises preventing transfer of at least a portion of the software to the current user device (col. 3, lines 16-49).

As per claim 32, it is disclosed by Ananda wherein the step of controlling access to the software comprises preventing the current user device from utilizing the software (col. 10, lines 13-15).

As per claim 35, it is taught by Ananda of further comprising encrypting the authentication code (col. 9, lines 25-34 and col. 10, line 63 through col. 11, line 8).

As per claim 36, it is disclosed by Ananda of further comprising encrypting the registration information (col. 9, lines 25-34).

As per claim 37, Ananda teaches of further comprising associating an identifier with the software to trigger authentication by an authorized representative entity (col. 10, lines 63 through col. 11, line 15).

As per claim 38, Ananda discloses of further comprising securing any means for generating the authentication code after generating the authentication code associated with the software (col. 10, line 63 through col. 11, line 15).

As per claim 39, it is taught by Ananda wherein the steps of obtaining registration information, generating an authentication code, and associating the authentication code are at least partially performed by a authorized representative entity, the method further

comprising: modifying the authorized representative entity to disable subsequent generation of authentication codes associated with the software (col. 10, lines 8-15). The teachings of Xu et al are relied upon for disclosing of the permitting offline (non-continuous connection) playback of digital content files which includes managing the related content rights (col. 2, lines 23-24), please refer above for the motivation of applying the aspect of offline validation as is disclosed by Xu et al. Slama is relied upon for disclosing of the use of a hardware based authorized representative entity that is installed on a computer (col. 3, lines 47-54 and col. 11, lines 53-56), please refer above for the motivation of applying the teachings of Slama.

As per claim 40, it is disclosed by Ananda wherein the steps of obtaining registration information, generating an authentication code, and associating the authentication code are performed by a remote authorized representative prior to distribution of the software (col. 3, lines 16-49).

As per claim 41, Ananda teaches of a method for securing software to reduce unauthorized use having an hardware based authorized representative entity installed on or in a user device, the method comprising determining whether the user device is authorized to access the software using the authorized representative entity; and controlling access to the software based on whether the user device is determined to be authorized (col. 3, lines 11-15 & 21-28; col. 4, lines 18-28; and col. 11, lines 9-13). The teachings of Ananda disclose of a continuous connection to the remote authorized representative entity, but fail to teach that the continuous connection to a remote authorized entity is not required and that the authorized representative entity is installed

in or on the user device. It is taught by Xu et al of permitting offline (non-continuous connection) playback of digital content files which includes managing the related content rights (col. 2, lines 23-24). Keys are retrieved by the end user's system and a license (authorized representative entity) is retrieved from a license server which is installed on the end user's system, the license is required for playback of the content file (col. 3, lines 11-19 and col. 5, lines 24-38). It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to apply localized validation of licensed software. The teachings of Xu et al disclose of motivation for applying localized validation by reciting of the need to protect digital information and management of digital rights in an offline environment (col. 2, lines 15-19). It is obvious that the teachings of Ananda would have benefited from validation of licensed software by using the authorized representative installed in or on the user's device whereby the authorized representative would then be able to valid the use of licensed software offline on an enduser's system as taught by Xu et al.

The combined teachings of Ananda and Xu et al fail to disclose that the authorized representative entity is hardware. It is taught by Slama of using a hardware based authorized representative entity that is installed on a computer (col. 3, lines 47-54 and col. 11, lines 53-56). It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to apply hardware based protection. The teachings of Slama recite of motivation of using a dedicated device to ensure that protected software is only executed on authorized computers (col. 2, lines 9-15). It is obvious that the combined teachings of Ananda and Xu et al would have

been further secured from unauthorized usage by requiring a hardware based representative to be used in order to dictate if software is authorized for execution on a particular computer as is disclosed by Slama.

As per claim 43, it is taught by Ananda of further comprising determining whether the user device is authorized to access the software using a remotely located authorized representative entity (col. 10, lines 4-15 and col. 11, lines 61-65). The teachings of Xu et al are relied upon for disclosing of the permitting offline (non-continuous connection) playback of digital content files which includes managing the related content rights (col. 2, lines 23-24), please refer above for the motivation of applying the aspect of offline validation as is disclosed by Xu et al. Slama is relied upon for disclosing of the use of a hardware based authorized representative entity that is installed on a computer (col. 3, lines 47-54 and col. 11, lines 53-56), please refer above for the motivation of applying the teachings of Slama.

As per claim 51, Ananda discloses wherein the step of determining whether the user device is authorized comprises comparing registration information associated with the user device to registration information associated with the software (col. 3, lines 16-49).

As per claim 52, it is taught by Ananda wherein the registration information associated with the software is embedded within an authentication code (col. 3, lines 24-28).

As per claim 53, it is disclosed by Ananda wherein the registration information associated with the software is encrypted (col. 11, line 61 through col. 12, line 14).

As per claim 54, Ananda teaches wherein the registration information includes hardware information (col. 9, lines 5-6).

As per claim 55, Ananda discloses wherein the registration information includes hardware information associated with a unique user device (col. 3, line 11-15).

As per claim 56, it is taught by Ananda wherein the hardware information includes a serial number (col. 8, lines 18-23).

As per claim 58, the teachings of Xu et al are relied upon for disclosing of the permitting offline (non-continuous connection) playback of digital content files which includes managing the related content rights and wherein the authorized representative entity is installed by a manufacturer of the user device (col. 2, lines 23-24), please refer above for the motivation of applying the aspect of offline validation as is disclosed by Xu et al. Slama is relied upon for disclosing of the use of a hardware based authorized representative entity that is installed on a computer (col. 3, lines 47-54 and col. 11, lines 53-56), please refer above for the motivation of applying the teachings of Slama.

As per claim 59, the teachings of Xu et al are relied upon for disclosing of the permitting offline (non-continuous connection) playback of digital content files which includes managing the related content rights and the authorized representative entity is installed from a computer readable storage medium (col. 2, lines 23-24), please refer above for the motivation of applying the aspect of offline validation as is disclosed by Xu et al. Slama is relied upon for disclosing of the use of a hardware based authorized representative entity that is installed on a computer (col. 3, lines 47-54 and col. 11, lines 53-56), please refer above for the motivation of applying the teachings of Slama.

As per claim 60, the teachings of Xu et al are relied upon for disclosing of the permitting offline (non-continuous connection) playback of digital content files which includes managing the related content rights and is downloaded to the user device (col. 2, lines 23-24), please refer above for the motivation of applying the aspect of offline validation as is disclosed by Xu et al. Slama is relied upon for disclosing of the use of a hardware based authorized representative entity that is installed on a computer (col. 3, lines 47-54 and col. 11, lines 53-56), please refer above for the motivation of applying the teachings of Slama.

As per claim 61, Xu et al discloses wherein the software is electronically distributed software across a network (col. 2, lines 23-24), please refer above for the motivation of applying the aspect of offline validation as is disclosed by Xu et al.

As per claim 62, Ananda discloses wherein the step of controlling access comprises preventing the software from being transferred to a second user device (col. 10, lines 8-15).

As per claim 63, it is taught by Ananda wherein the step of controlling access comprises preventing the software from being executed by the user device (col. 10, lines 8-15).

As per claim 64, it is disclosed by Ananda wherein the step of controlling access comprises providing limited access to the software (col. 10, lines 8-15).

As per claim 65, Ananda teaches wherein the software comprises data representing content selected from the group consisting of music, video, an application

program, an operating system component, a game, a movie, graphics, watermarked works, a magazine, and a book (col. 1, lines 17-19).

As per claim 66, Ananda discloses wherein the software comprises instructions for generating at least one authentication code at least partially based on registration information associated with the user device (col. 11, lines 9-13).

As per claim 67, it is taught by Ananda wherein the software comprises instructions for encrypting the authentication code (col. 9, lines 25-34 and col. 10, line 63 through col. 11, line 8).

As per claim 68, it is disclosed by Ananda wherein the step of determining whether the user device is authorized comprises contacting a remote authorized representative entity if the authorized representative entity is unable to determine whether the user device is authorized (col. 10, lines 8-15). The teachings of Xu et al are relied upon for disclosing of the permitting offline (non-continuous connection) playback of digital content files which includes managing the related content rights (col. 2, lines 23-24), please refer above for the motivation of applying the aspect of offline validation as is disclosed by Xu et al.

As per claim 69, Ananda teaches wherein the step of determining whether the user device is authorized comprises contacting a remote authorized representative if the authorized representative determines that the user device is not authorized (col. 10, lines 8-15). The teachings of Xu et al are relied upon for disclosing of the permitting offline (non-continuous connection) playback of digital content files which includes

managing the related content rights (col. 2, lines 23-24), please refer above for the motivation of applying the aspect of offline validation as is disclosed by Xu et al.

As per claim 70, Ananda discloses wherein the step of determining whether the user device is authorized comprises obtaining registration information associated with the user device and comparing the registration information associated with the user device with registration information encoded in an authentication code associated with the software (col. 3, lines 22-29 and col. 10, lines 8-15).

As per claim 72, it is disclosed by Ananda of further comprising automatically contacting a remote authorized representative based upon a triggering event to receive information (col. 4, line 61 through col. 5, line 10).

As per claim 73, Ananda teaches wherein the information is selected from a group consisting of updates, upgrades, patches, marketing information, promotional information, quality assurance information, network monitoring and metering information, and error and usage information (col. 20, lines 53-62).

As per claim 74, Ananda discloses wherein the information updates the authorized representative (col. 20, lines 53-62). The teachings of Xu et al are relied upon for disclosing of the permitting offline (non-continuous connection) playback of digital content files which includes managing the related content rights (col. 2, lines 23-24), please refer above for the motivation of applying the aspect of offline validation as is disclosed by Xu et al.

As per claim 75, it is taught by Ananda wherein the information modifies the software (col. 10, lines 8-15 and col. 20, lines 53-62).

As per claim 76, it is disclosed by Ananda wherein the triggering event is based on a user action (col. 3, lines 21-28).

As per claim 77, Ananda teaches wherein the automatic contact with the remote authorized representative is repeated (col. 10, lines 8-15).

5. Claims 26-28,33,34,57, and 66 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ananda, U.S. Patent 5,495,411 in view of Xu et al, U.S. Patent 6,915,425 in further view of Slama, U.S. Patent 6,665,799 in further view of Barber et al, U.S. Patent 5,390,297.

As per claim 26, Ananda teaches wherein the authentication code corresponds to a user device (col. 3, lines 11-15). The combined teachings fail to disclose of a transferring software to a secondary device. It is taught by Barber et al that licensed software can be used on multiple workstations (secondary devices) and authorized is checked to see if the transfer is permitted (col. 2, lines 21-36 & 49-67). It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to allow multiple copies of licensed software to be used on different computers. The teachings of Barber et al disclose of motivation for doing so by reciting of the need to manage licenses that are to be run on multiple nodes (secondary devices) and to limit the number of copies of a program the are executing simultaneously on the nodes of a network which in turn protects the vendors protected software from being illicitly used (col. 2, lines 6-9 and col. 3, lines 30-42). It is obvious that the combined teachings of Ananda, Xu et al, and Slama would have allowed the

incorporation of Barber et al and the feature of limiting the simultaneous copies to authorized computers.

As per claim 27, Ananda discloses wherein the authentication code at least partially corresponds to a manufacturer of a user device (col. 9, lines 5-6).

As per claim 28, it is taught by Ananda wherein the authentication code at least partially corresponds to a model of a user device (col. 9, lines 5-6).

As per claim 33, Ananda teaches wherein the steps of determining and controlling are at least partially performed by an authorized representative (col. 10, lines 4-15). The teachings of Xu et al are relied upon for disclosing of the permitting offline (non-continuous connection) playback of digital content files which includes managing the related content rights (col. 2, lines 23-24), please refer above for the motivation of applying the aspect of offline validation as is disclosed by Xu et al. The combined teachings fail to disclose of a transferring software to a secondary device. It is taught by Barber et al that licensed software can be used on multiple workstations (secondary devices) and authorized is checked to see if the transfer is permitted (col. 2, lines 21-36 & 49-67). It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to allow multiple copies of licensed software to be used on different computers. The teachings of Barber et al disclose of motivation for doing so by reciting of the need to manage licenses that are to be run on multiple nodes (secondary devices) and to limit the number of copies of a program the are executing simultaneously on the nodes of a network which in turn protects the vendors protected software from being illicitly used (col. 2, lines 6-9 and col. 3, lines 30-42). It is obvious

that the combined teachings of Ananda and Xu et al would have allowed the incorporation of Barber et al and the feature of limiting the simultaneous copies to authorized computers.

As per claim 34, Ananda discloses wherein the steps of obtaining, generating, and associating are performed by a primary user device (col. 10, lines 4-15). The combined teachings fail to disclose of a transferring software to a secondary device which determined if usage is permitted. It is taught by Barber et al that licensed software can be used on multiple workstations (secondary devices) and authorized is checked to see if the transfer is permitted (col. 2, lines 21-36 & 49-67). It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to allow multiple copies of licensed software to be used on different computers. The teachings of Barber et al disclose of motivation for doing so by reciting of the need to manage licenses that are to be run on multiple nodes (secondary devices) and to limit the number of copies of a program the are executing simultaneously on the nodes of a network which in turn protects the vendors protected software from being illicitly used (col. 2, lines 6-9 and col. 3, lines 30-42). It is obvious that the combined teachings of Ananda and Xu et al would have allowed the incorporation of Barber et al and the feature of limiting the simultaneous copies to authorized computers.

As per claims 57 and 66, Ananda teaches wherein the registration information includes hardware information associated with a devices (col. 3, lines 11-15). The combined teachings fail to disclose of a transferring software to a secondary device. It

is taught by Barber et al that licensed software can be used on multiple workstations (secondary devices) and authorized is checked to see if the transfer is permitted (col. 2, lines 21-36 & 49-67). It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to allow multiple copies of licensed software to be used on different computers. The teachings of Barber et al disclose of motivation for doing so by reciting of the need to manage licenses that are to be run on multiple nodes (secondary devices) and to limit the number of copies of a program the are executing simultaneously on the nodes of a network which in turn protects the vendors protected software from being illicitly used (col. 2, lines 6-9 and col. 3, lines 30-42). It is obvious that the combined teachings of Ananda, Xu et al, and Slama would have allowed the incorporation of Barber et al and the feature of limiting the simultaneous copies to authorized computers.

6. Claim 71 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ananda, U.S. Patent 5,495,411 in view of Xu et al, U.S. Patent 6,915,425 in further view of Slama, U.S. Patent 6,665,799 in further view of Grundy, U.S. Patent 5,291,598.

As per claim 71, it is taught by Ananda of further comprising detecting an identifier associated with the software to trigger authentication functions performed by the authorized representative entity; and performing the steps of determining whether the user device is authorized and controlling access to the software only if the identifier is detected (col. 10, lines 8-15). The teachings of Xu et al are relied upon for disclosing

of the permitting offline (non-continuous connection) playback of digital content files which includes managing the related content rights (col. 2, lines 23-24), please refer above for the motivation of applying the aspect of offline validation as is disclosed by Xu et al. Slama is relied upon for disclosing of the use of a hardware based authorized representative entity that is installed on a computer (col. 3, lines 47-54 and col. 11, lines 53-56), please refer above for the motivation of applying the teachings of Slama.

The combined teachings fail to disclose of allowing the software to function if authorization is not detected based on an identifier not being detected. It is disclosed by Grundy of ownership details records being reviewed and if there is no information in regards to a full-function mode, the software will continue to operate (col. 5, lines 39-49). It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to apply controls for dictating software usage requirements. The teachings of Grundy recite of motivational benefits by disclosing of the need to permit consumers to evaluate products more efficient and to provide for means to protect against privacy (col. 4, lines 9-18). It is obvious the combined teachings would have benefited from the disclosure of Grundy in that further protection would have been added by allowing software to function even if not in a fully operational mode.

7. Claims 78 and 80-99 rejected under 35 U.S.C. 103(a) as being unpatentable over Ananda, U.S. Patent 5,495,411 in view of Grundy, U.S. Patent 5,291,598, in further view of Xu et al, U.S. Patent 6,915,425.

As per claim 78, Ananda discloses of a method for reducing unauthorized use of software, the method comprising associating at least one identifier with the software corresponding to a request for digital rights management; distributing the software to a user; detecting the at least one identifier using an authorized representative entity; associating at least one authentication code with the software; determining whether a user device is authorized to access the software; and controlling access to the software based on whether the user device is authorized (col. 3, lines 11-15 & 21-28; col. 4, lines 18-28; and col. 11, lines 9-13). The teachings of Ananda fail to disclose of allowing the software to function if authorization is not detected based on an identifier not being detected. It is disclosed by Grundy of ownership details records being reviewed and if there is no information in regards to a full-function mode, the software will continue to operate (col. 5, lines 39-49). It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to apply controls for dictating software usage requirements. The teachings of Grundy recite of motivational benefits by disclosing of the need to permit consumers to evaluate products more efficient and to provide for means to protect against privacy (col. 4, lines 9-18). It is obvious the teachings of Ananda would have benefited from the disclosure of Grundy in that further protection would have been added by allowing software to function even if not in a fully operational mode.

The teachings of Ananda disclose of a continuous connection to the remote authorized representative entity and the combined teachings fail to teach that the continuous connection to a remote authorized entity is not required and that the

authorized representative entity is installed in or on the user device. It is taught by Xu et al of permitting offline (non-continuous connection) playback of digital content files which includes managing the related content rights (col. 2, lines 23-24). Keys are retrieved by the end user's system and a license (authorized representative entity) is retrieved from a license server which is installed on the end user's system, the license is required for playback of the content file (col. 3, lines 11-19 and col. 5, lines 24-38). It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to apply localized validation of licensed software. The teachings of Xu et al disclose of motivation for applying localized validation by reciting of the need to protect digital information and management of digital rights in an offline environment (col. 2, lines 15-19). It is obvious that the teachings of Ananda would have benefited from validation of licensed software by using the authorized representative installed in or on the user's device whereby the authorized representative would then be able to valid the use of licensed software offline on an enduser's system as taught by Xu et al.

As per claim 80, it is disclosed by Ananda of further comprising encrypting the at least one authentication code (col. 9, lines 25-34 and col. 10, line 63 through col. 11, line 8).

As per claim 81, Ananda teaches of further comprising obtaining registration information associated with at least one user device; and generating the at least one authentication code at least partially based on the registration information (col. 3, lines 21-28).

As per claim 82, Ananda discloses of further comprising encrypting the registration information (col. 11, line 61 through col. 12, line 14).

As per claim 83, it is taught by Ananda wherein the steps of obtaining registration information, generating the at least one authentication code, and associating the at least one authentication code are performed before the step of distributing the software (col. 3, lines 11-31).

As per claim 84, it is disclosed by Ananda wherein the steps of obtaining registration information, generating the at least one authentication code, and associating the at least one authentication code are performed substantially concurrently with the step of distributing the software (col. 3, lines 11-31).

As per claim 85, Ananda teaches wherein the steps of obtaining registration information, generating the at least one authentication code, and associating the at least one authentication code are performed subsequent to the step of distributing the software (col. 3, lines 11-31).

As per claim 86, Ananda discloses wherein the steps of obtaining registration information, generating the at least one authentication code, and associating the at least one authentication code are performed by an authorized representative entity (col. 3, lines 11-31; col. 10, lines 4-15; and col. 11, lines 61-65). The teachings of Xu et al are relied upon for disclosing of the permitting offline (non-continuous connection) playback of digital content files which includes managing the related content rights (col. 2, lines 23-24), please refer above for the motivation of applying the aspect of offline validation as is disclosed by Xu et al.

As per claim 87, Ananda teaches wherein the step of generating the at least one authentication code is performed by an authorized representative entity, the method further comprising securing the authentication code to resist user tampering (col. 11, lines 9-13). The teachings of Xu et al are relied upon for disclosing of the permitting offline (non-continuous connection) playback of digital content files which includes managing the related content rights (col. 2, lines 23-24), please refer above for the motivation of applying the aspect of offline validation as is disclosed by Xu et al.

As per claim 88, Ananda discloses wherein the step of securing comprises preventing the authorized representative entity from generating any more authentication codes for the software (col. 10, lines 4-15 and col. 11, lines 61-65). The teachings of Xu et al are relied upon for disclosing of the permitting offline (non-continuous connection) playback of digital content files which includes managing the related content rights (col. 2, lines 23-24), please refer above for the motivation of applying the aspect of offline validation as is disclosed by Xu et al.

As per claim 89, it is taught by Ananda wherein the step of securing comprises encrypting the authentication code (col. 9, lines 25-34 and col. 10, line 63 through col. 11, line 8).

As per claim 90, the teachings of Xu et al are relied upon for disclosing of the permitting offline (non-continuous connection) playback of digital content files which includes managing the related content rights and installing an authorized representative entity on or in the user device if an operational authorized representative entity is not

available locally (col. 2, lines 23-24), please refer above for the motivation of applying the aspect of offline validation as is disclosed by Xu et al.

As per claim 91, Xu et al teaches wherein the step of installing comprises transferring the authorized representative entity to the user device from a remote authorized representative entity (col. 2, lines 23-24), please refer above for the motivation of applying the aspect of offline validation as is disclosed by Xu et al.

As per claim 92, it is taught by Xu et al wherein the software is transferred directly to a user device from a local computer readable storage medium software (col. 2, lines 23-24), please refer above for the motivation of applying the aspect of offline validation as is disclosed by Xu et al.

As per claim 93, it is taught by Xu et al wherein the software includes an authorized representative entity and wherein the step of installing comprises transferring the authorized representative entity to the user device from the software (col. 2, lines 23-24), please refer above for the motivation of applying the aspect of offline validation as is disclosed by Xu et al.

As per claim 94, it is disclosed by Xu et al of determining whether an operational authorized representative entity is installed on or in the user device; and contacting a remote authorized representative entity if no operational authorized representative entity is installed on or in the user device (col. 2, lines 23-24), please refer above for the motivation of applying the aspect of offline validation as is disclosed by Xu et al.

As per claim 95, Ananda teaches wherein the remote authorized representative entity performs the steps of determining whether a user device is authorized and controlling access to the software (col. 10, lines 8-15).

As per claim 96, Ananda discloses of further comprising obtaining registration information including hardware specific information associated with a user device, wherein the steps of obtaining registration information and associating at least one authentication code are performed prior to the step of distributing the software to a user (col. 3, lines 22-29 and col. 10, lines 8-15).

As per claim 97, it is taught by Ananda of further comprising obtaining registration information including hardware specific information associated with a user device, wherein the steps of obtaining registration information and associating at least one authentication code are performed substantially concurrently with the step of distributing the software to a user (col. 3, lines 22-29 and col. 10, lines 8-15).

As per claim 98, it is disclosed by Ananda of further comprising obtaining registration information including hardware specific information associated with a user device, wherein the steps of obtaining registration information and associating at least one authentication code are performed following the step of distributing the software to a user (col. 3, lines 22-29 and col. 10, lines 8-15).

As per claim 99, Ananda teaches wherein the step of controlling access to the software comprises preventing the software from being transferred to the user device if the user device is not authorized (col. 10, lines 8-15).

8. Claim 79 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ananda, U.S. Patent 5,495,411 in view of Grundy, U.S. Patent 5,291,598, in further view of Xu et al, U.S. Patent 6,915,425 in further view of Slama, U.S. Patent 6,665,799.

As per claim 79, it is taught by Xu et al of determining whether an operational authorized representative entity is installed on or in the user device; and contacting a remote authorized representative entity if no operational authorized representative entity is installed on or in the user device (col. 2, lines 23-24), please refer above for the motivation of applying the aspect of offline validation as is disclosed by Xu et al. The combined teachings fail to disclose that the authorized representative entity is hardware. It is taught by Slama of using a hardware based authorized representative entity that is installed on a computer (col. 3, lines 47-54 and col. 11, lines 53-56). It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to apply hardware based protection. The teachings of Slama recite of motivation of using a dedicated device to ensure that protected software is only executed on authorized computers (col. 2, lines 9-15). It is obvious that the combined teachings would have been further secured from unauthorized usage by requiring a hardware based representative to be used in order to dictate if software is authorized for execution on a particular computer as is disclosed by Slama.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher A. Revak whose telephone number is 571-272-3794. The examiner can normally be reached on Monday-Friday, 9:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Christopher A. Revak/
Primary Examiner, Art Unit 2131